REMARKS

Claims 1, 7, 13, 18, 22 and 26 are amended. Claims 1-31 remain in the application for consideration. In view of the following remarks, Applicant respectfully requests reconsideration and allowance of the subject application.

Drawing Objections

The drawings are objected to because the margins are out of specification in Fig. 2. Applicant submits herewith a new drawing sheet for Fig. 2 which corrects the margins. Applicant thanks the Office for the Office's attention to detail.

35 U.S.C. §§ 102 and 103 Rejections

Claims 1-11 and 13-30 stand rejected under 35 U.S.C. § 102(a) as being anticipated by U.S. Patent No. 5,884,033 to Duvall et al (hereinafter, "Duvall"). Claims 12 and 31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Duvall in view of Oliver et al., "Building a Windows NT 4 Internet Server", 1996, p. 203.

The Duvall Reference

The reference to **Duvall** discloses a client-based filtering system. The system allows a user to filter material received over the Internet that is personally objectionable, whether that material is sexually explicit, violent, politically extreme, or otherwise, depending on the user's individual tastes and sensitivities.

The filter compares portions of incoming and/or outgoing messages to filtering information in a filter database and determines whether to block or allow incoming and/or outgoing transmissions of messages in response to the

comparison. In response to a match between the portion of the message and the filtering information, the system can employ one of a number of different specified blocking options. The system has an update server that is accessible over the Internet and that has new filtering information for updating the filter database.

Claims 1-6

Claim 1 has been amended and recites a Web server input string screening method comprising [added language appears in bold italics]:

- determining an attack pattern that can be used to attack a Web server, *the attack pattern comprising content that is designed to constitute one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server*;
- defining a search pattern that can be used to detect the attack pattern, the search pattern being defined in a manner that permits variability among its constituent parts;
- receiving an input string that is intended for use by a Web server;
- evaluating the input string using the search pattern to ascertain whether the attack pattern is present; and
- implementing a remedial action if an attack pattern is found that matches the search pattern.

In the Office Action, the Office rejects this claim under 35 U.S.C. § 102 and argues that Duvall anticipates the claimed subject matter. Specifically, the Office argues that Duvall "defines a plurality of unwanted input strings to be filtered (see column 3, line 64 to column 4, line 11), a search pattern that permits variability, can search a portion of the string, and has wildcard characters (see column 6, lines 28-42), receives an input string on a web server (see column 8, lines 18-27), evaluates the strings, and takes remedial action if necessary, including denying the request (see column 6, line 60 to column 7, line 13)."

In the previous Response, Applicant argued that Duvall did not anticipate this claim. Applicant pointed out that according to MPEP § 706.02, "for anticipation under 35 U.S.C. 102, the reference must teach *every aspect* of the claimed invention either explicitly or impliedly. Any feature not directly taught must be *inherently present*."

Applicant argued that the first element of claim 1 recites "determining an *attack pattern* that can be used to *attack a web server*." Applicant pointed out that Duvall did not disclose this; and, in fact, the Office did not even *cite* Duvall for this feature. Applicant previously argued and maintains that Duvall's disclosure actually has absolutely *nothing* to do with Web server attacks. Instead, Duvall's disclosure deals with a system in which a user can filter material received over the Internet that is *personally objectionable*, whether that material is sexually explicit, violent, politically extreme, or otherwise, depending on that user's *individual tastes and sensitivities*. This is very different from and not to be confused with determining an *attack pattern* that can be used to *attack a Web server*.

Further, in responding to Applicant's arguments, the Office argues that "attack patterns can *only* be defined as being undesired strings that are intended for the web server." See, Office Action, page 5. Applicant very respectfully disagrees with the Office and submits that the Office has ignored germane claim language that appears in claim 1. Specifically, claim 1 recites, *inter alia,* that the attack pattern "can be used to attack a Web server." Thus, attack patterns as recited in claim 1 cannot simply be viewed *only* as undesired strings as argued by the Office. Rather, attack patterns, as that term is used in the present claim, must be viewed by the Office as a pattern that "can be used to attack a Web server."

The Office further argues that "applicant's alleged difference is in the subjective intent of the creator of the strings rather than in the content or processing of the strings." See, Office Action, page 6. Applicant very respectfully submits that this is simply not the case. Claim 1 very specifically recites an attack pattern and defines the attack pattern as one that "can be used to attack a Web server."

Nonetheless, and in a sincere attempt to advance prosecution of this application, Applicant has amended claim 1 to clarify the content of the recited attack pattern. Specifically, this claim has been amended to recite that the attack pattern comprises "content that is designed to constitute one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server." Support for this amendment can be found in the Specification. Applicant respectfully submits that with this clarification, the content of Applicant's recited attack pattern is clear and, when taken in combination with the remainder of the claim, recites a method that is neither disclosed nor suggested by Duvall, either singly or in combination with any of the references of record. Accordingly, for at least this reason, this claim is allowable.

Claims 2-6 depend either directly or indirectly from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither disclosed nor taught by the references of record, either singly or in combination with one another.

Claims 7-12

Claim 7 has been amended and recites a Web server input string screening method comprising [added language appears in bold italics]:

- defining one or more search patterns that comprise literal characters and special characters, wherein the literal characters indicate exact characters in an input string that is intended for receipt by a Web server, and the special characters indicate variable characters in an input string that is intended for receipt by the Web server, the search patterns being usable to search for an attack pattern that can be used to attack the Web server, *the attack pattern comprising content that is designed to constitute one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server*; and
- storing the one or more search patterns in a memory location that is accessible to a screening tool for evaluating an input string that is intended for receipt by the Web server.

In making out the rejection of this claim, the Office again argues that Duvall anticipates this claim. Once more, Applicant respectfully submits that Duvall does not anticipate this claim. As noted above, Duvall discloses *nothing* of search patterns that are useable to search for an *attack pattern* that can be used to *attack a Web server*. Moreover, Duvall does not even *suggest* any sort of method whatsoever for dealing with attack patterns, let alone their use in connection with a Web server.

Nonetheless, and in a sincere attempt to advance prosecution of this application, Applicant has amended claim 7 to clarify the content of the recited attack pattern. Specifically, this claim has been amended to recite that the attack pattern comprises "content that is designed to constitute one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server." Support for this amendment can be found in the Specification. Applicant

respectfully submits that with this clarification, the content of Applicant's recited attack pattern is clear and, when taken in combination with the remainder of the claim, recites a method that is neither disclosed nor suggested by Duvall, either singly or in combination with any of the references of record. Accordingly, for at least this reason, this claim is allowable.

Claims 8-12 depend from claim 7 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 7, are neither disclosed nor taught by the references of record, either singly or in combination with one another.

In addition, with respect to claim 12, which is rejected in view of Oliver, that reference is not seen to add anything of significance given the allowability of this claim and the failure of Duvall to anticipate or render obvious claim 7.

Claims 13-17

Claim 13 has been amended and recites a Web server input string screening method comprising [added language appears in bold italics]:

- defining one or more search patterns that are specified as a regular expression, the search patterns being usable to search for an attack pattern that can be used to attack the Web server, *the attack pattern comprising content that is designed to constitute one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server*; and
- storing the one or more search patterns in a memory location that is accessible to a screening tool for evaluating an input string that is intended for receipt by the Web server.

Again, the Office rejects this claim under § 102 by arguing that Duvall

discloses that "the search patterns may be stored in RAM." The Office cites to

column 4, lines 45-49, which are reproduced below:

> The system then checks for and retrieves any filters that match the
> particular IP address. The retrieved filters are checked to determine
> if any require immediate action, i.e., if unconditional allowing or
> blocking is required (steps 104, 106).

Applicant respectfully submits that Duvall neither discloses nor suggests

the subject matter of this claim. Specifically, Duvall neither discloses nor suggests

search patterns that are usable to search for attack patterns that can be used to

attack a Web server.

Nonetheless, and in a sincere attempt to advance prosecution of this

application, Applicant has amended claim 13 to clarify the content of the recited

attack pattern. Specifically, this claim has been amended to recite that the attack

pattern comprises "content that is designed to constitute one or more of a

disclosure attack, an integrity attack or a denial of service attack on the Web

server." Support for this amendment can be found in the Specification. Applicant

respectfully submits that with this clarification, the content of Applicant's recited

attack pattern is clear and, when taken in combination with the remainder of the

claim, recites a method that is neither disclosed nor suggested by Duvall, either

singly or in combination with any of the references of record. Accordingly, for at

least this reason, this claim is allowable.

Claims 14-17 depend from claim 13 and are allowable as depending from

an allowable base claim. These claims are also allowable for their own recited

features which, in combination with those recited in claim 13, are neither disclosed

nor taught by the references of record, either singly or in combination with one another.

Claims 18-21

Claim 18 has been amended and recites a Web server input string screening tool embodied on a computer-readable medium comprising [added language appears in bold italics]:

- a pattern matching engine that is configured to receive an input string that is intended for use by a Web server and evaluate the input string to ascertain whether it likely constitutes an attack on the Web server, *the attack comprising one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server*; and
- one or more patterns that are usable by the pattern matching engine to evaluate the input string, the patterns being defined in a manner that permits variability among the constituent parts of the one or more patterns.

The Office rejects this claim, again citing Duvall. Applicant respectfully traverses the rejection. Duvall neither discloses nor suggests a pattern matching engine that is configured to evaluate an input string to ascertain *whether it likely constitutes an attack on a Web server*.

Nonetheless, and in a sincere attempt to advance prosecution of this application, Applicant has amended claim 18 to clarify that the attack can comprise "one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server." Support for this amendment can be found in the Specification. Applicant respectfully submits that with this clarification, this claim recites a method that is neither disclosed nor suggested by Duvall, either

singly or in combination with any of the references of record. Accordingly, for at least this reason, this claim is allowable.

Claims 19-21 depend from claim 18 either directly or indirectly and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 18, are neither disclosed nor taught by the references of record, either singly or in combination with one another.

Claims 22-25

Claim 22 has been amended and recites one or more computer readable media having computer-readable instructions thereon which, when executed by a computer perform the following steps [added language appears in bold italics]:

- receiving an input string that is intended for use by a Web server;
- evaluating the input string using a search pattern to ascertain whether the input string contains an attack pattern that can be used to attack the Web server, *the attack pattern comprising content that is designed to constitute one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server*, the search pattern comprising literal characters and special characters, wherein literal characters indicate exact characters in the input string, and the special characters indicate variable characters in the input string; and
- implementing a remedial action if an attack pattern is found that matches the search pattern.

In making out the rejection of this claim, the Office again cites Duvall. However, Duvall does not disclose or suggest the act of evaluating an input string using a search pattern to ascertain whether the input string contains an *attack pattern* that can be used to *attack a Web server*. Because Duvall does not teach or

suggest such an evaluation, it cannot possibly disclose implementing a remedial action if an *attack pattern* is found that matches the search pattern.

Nonetheless, and in a sincere attempt to advance prosecution of this application, Applicant has amended claim 22 to clarify the content of the recited attack pattern. Specifically, this claim has been amended to recite that the attack pattern comprises "content that is designed to constitute one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server." Support for this amendment can be found in the Specification. Applicant respectfully submits that with this clarification, the content of Applicant's recited attack pattern is clear and, when taken in combination with the remainder of the claim, recites a method that is neither disclosed nor suggested by Duvall, either singly or in combination with any of the references of record. Accordingly, for at least this reason, this claim is allowable.

Claims 23-25 depend either directly or indirectly from claim 22 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 22, are neither disclosed nor taught by the references of record, either singly or in combination with one another.

Claims 26-31

Claim 26 has been amended and recites a collection of Web server screening patterns embodied on a computer-readable medium comprising [added language appears in bold italics]:

- a memory; and
- a plurality of patterns stored in the memory, the patterns being useable to screen input strings that are intended for use by a Web server *to ascertain whether the input strings comprise attack patterns, the attack patterns comprising content that is designed to constitute one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server,* individual patterns being defined in a manner that permits variability among their constituent parts.

Again, the Office rejects the claim under § 102 by arguing that Duvall discloses that "the search patterns may be stored in RAM." The Office cites to column 4, lines 45-49, which was reproduced earlier.

This claim has been amended to clarify that the attack patterns comprise "content that is designed to constitute one or more of a disclosure attack, an integrity attack or a denial of service attack on the Web server." As discussed in the previous response, Duvall does not disclose attack patterns. With the clarification provided by the present amendment, this claim clearly recites subject matter that is neither disclosed nor suggested by Duvall either singly or in combination with any of the references of record. Accordingly, this claim is allowable.

Claims 27-31 depend from claim 26 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 26, are neither disclosed

nor taught by the references of record, either singly or in combination with one another.

In addition, with respect to claim 31, which is rejected in view of Oliver, that reference is not seen to add anything of significance given the allowability of claim 26.

Conclusion

Applicant has made a sincere attempt to advance prosecution in this application. Applicant respectfully submits that all of the claims are in condition for allowance and Applicant respectfully requests a Notice of Allowability be issued forthwith. If the next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully Submitted,

Dated: 3/24/04

By: _____
Lance R. Sadler
Reg. No. 38,605
(509) 324-9256